IN THE SPECIFICATION

Please amend the paragraph at page 53, lines 2-14, as follows:

As for (1), for example, an S-box 1001 in the first-half of the preceding extended S-box and an S-box 1002 in the first-half of the succeeding extended S-box 103 are interconnected by two paths indicated by bold lines as shown in FIG. 35. Other S-boxes are also interconnected by two to four paths. In contrast, with the conventional SQUARE encryption/Rijndael encryption, an S-box ~~1001~~ 1003 in the first-half of the preceding extended S-box and an S-box ~~1002~~ 1004 in the first-half of the succeeding extended S-box 103 are interconnected by only one path (fan-in=1) as shown in FIG. 36 and the same is true of other S-boxes. Therefore, the avalanche effect is low.